IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

MONIQUE CASTRO, ANDREW GILSEY, ANNA HAMILTON, ANNA PALAFOX, LATOYA PETTUS, TINA SALINAS, and TINA YOUNG, individually, and on behalf of all others similarly situated, Plaintiffs, vs. AT&T, INC., Defendant.	Case No. 3:24-cv-01992 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Monique Castro ("Castro"), Andrew Gilsey ("Gilsey"), Anna Hamilton ("Hamilton"), Anna Palafox ("Palafox"), Latoya Pettus ("Pettus"), Tina Salinas ("Salinas"), and Tina Young ("Young"), (collectively "Plaintiffs"), individually, and on behalf of the class defined below, bring this class action complaint against AT&T, Inc., ("AT&T" or "Defendant") and allege on personal knowledge as to themselves, and on information and belief as to all other allegations, as follows:

INTRODUCTION

1. Plaintiffs bring this action against AT&T for its failure to properly and adequately safeguard the personally identifying information ("PII") of tens of millions of current and former AT&T customers.

2. Defendant AT&T is a telecommunications provider headquartered in Dallas, Texas. AT&T provides consumer and business cellular, internet, and other telecommunications services throughout the United States. AT&T arose from the Bell Telephone Company, founded in 1877 by Alexander Graham Bell. Over the course of nearly one hundred and fifty years and after a series of mergers and acquisitions in the telecommunication industry, AT&T has grown into the largest telecommunications company in the United States, with a market share of approximately 46% of wireless subscriptions.

3. U.S. telecommunications companies are a lucrative target for hackers and cyber-thieves.

4. At all relevant times, Defendant was aware of the risks of a data breach and that it would be specifically targeted by malicious hackers. Indeed, in 2021, AT&T competitor T-Mobile was the subject of a massive data breach involving the same critical PII, names, birth dates, and Social Security Numbers, that are at issue here.[1]

5. Armed with the PII from these records, hackers can sell the PII to other thieves or misuse the PII themselves to commit a variety of crimes that harm victims of the Data Breach. For instance, they can take out loans, mortgage property, open financial accounts, and open credit cards

[1] https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation, last visited August 2, 2024.

in a victim's name; use a victim's information to obtain government benefits; or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in another person's name; or give false information to police during an arrest.

6. As a requirement of providing services, AT&T collects critical information from consumers, including, but not limited to, their names, email addresses, mailing addresses, birth dates, and Social Security Numbers: ("Private Information" or "PII").

7. On or about March 30, 2024, AT&T posted a notice on its website stating that "a number of AT&T passcodes have been compromised."[2] The notice further stated that "we will be communicating with current and former account holders with compromised sensitive personal information," but provided no specifics about what "sensitive personal information" was involved (the "Data Breach").[3] AT&T confirmed that a "data set" consisting of data relating to 7.6 million current AT&T customers and approximately 65.4 million former account holders had been released on the dark web approximately two weeks prior.[4,5,6] AT&T further acknowledged that this "data set" included critical PII such as names, Social Security numbers, email addresses, mailing addresses, phone numbers, and birth dates.

8. News reports further indicate that this "data set" appears to relate to a data breach that occurred several years earlier, in 2021, but was never acknowledged or remedied in any way by AT&T.[7] *Id.* At least one news outlet reports that AT&T disputes this claim, yet the Company has failed to explain to Plaintiffs and Class Members who is responsible for the Data Breach and when

---

[2] *See* https://www.att.com/support/article/my-account/000101995?bypasscache=1, last visited August 2, 2024.

[3] *Id.*

[4] https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html, last visited August 2, 2024.

[5] *See https://fortune.com/2024/03/31/att-data-breach-over-70-million-dark-web/*, last visited August 2, 2024.

[6] https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web, last visited August 2, 2024.

[7] https://techcrunch.com/2024/03/22/att-customers-data-leak-online/?guccounter=1, last visited August 2, 2024.

it occurred.[8] Notably, in 2021, when data purported to be from this 2021 breach surfaced, AT&T denied that it had been breached. *Id.* Similarly, on March 22, 2024, when *TechCrunch* initially reported on the release of AT&T data on the dark web, AT&T stated "We have no indications of a compromise of our systems. We determined in 2021 that the information offered on this online forum did not appear to have come from our systems. This appears to be the same dataset that has been recycled several times on this forum." *Id.*

9. AT&T has had a history of ongoing and significant data breaches over a number of years. Clearly, AT&T has still not addressed cyber-security and continues to remain open to attack as a consequence of its failure to institute and maintain adequate cyber-security measures, despite its obligation to do so. Even as recently as July 12, 2024, AT&T announced yet another massive data breach – this time respecting customer call and text records of tens of millions of consumers. The Federal Communications Commission has commenced an investigation.

10. Plaintiffs seek to hold Defendant responsible for its failure to protect and keep secure the PII of Plaintiffs and similarly situated Class Members and seek injunctive relief necessary to avoid further harm.

11. Plaintiffs further seek to hold Defendant responsible for its egregious failure to (a) identify the Data Breach, (b) identify its extent, and (c) promptly notify consumers.

12. As a result of Defendant's willful failure to prevent the Data Breach, Plaintiffs and Class Members are more susceptible to identity theft and have experienced, will continue to experience, and face an increased risk of financial harms, in that they are at substantial risk of identity theft, fraud, and other harm.

PARTIES

Plaintiff Anna Hamilton

13. Plaintiff Anna Hamilton is a resident of St. Johns and was, at all relevant times, a citizen of the state of Florida.

[8] https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web, last visited August 2, 2024.

14. Plaintiff Anna Hamilton is a consumer who has had a cellular phone account with Defendant for more than ten years and who has maintained broadband internet service with Defendant for approximately one year.

15. As a condition of obtaining services from AT&T, Plaintiff Hamilton was required to provide her PII to AT&T. Defendant used that PII to facilitate its provision of services and operate its business.

16. Plaintiff provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiffs' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

17. Plaintiff received a Notice of Data Breach in April 2024.

18. On information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

19. And in the aftermath of the Data Breach, Plaintiff has experienced multiple attempts at financial fraud including fraudulent charges posted to the credit card that Plaintiff uses to pay bills from AT&T. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft.

20. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

21. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiffs' PII right in the hands of criminals.

22. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries. Today, Plaintiff has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Monique Castro

23. Plaintiff Monique Castro is and at all times relevant was, a resident of Fresno and a citizen of the state of California.

24. Plaintiff Castro is a consumer who has had a cellular phone account with Defendant approximately seven years and who has maintained broadband internet service with Defendant for approximately four years.

25. As a condition of receiving services from Defendant, Plaintiff Castro was required to provide her PII, including her full name, address, phone number, date of birth, and Social Security Number, to Defendant. Defendant used that PII to facilitate its provision of services and operate its business.

26. Plaintiff provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiffs' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

27. Plaintiff received a Notice of Data Breach on April 25, 2024.

28. On information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

29. Plaintiff Castro has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Plaintiff Castro has also spent money out of pocket on monitoring services and software.

30. Plaintiff Castro fears for her personal financial security and worries about what information was exposed in the Data Breach.

31. Plaintiff suffered imminent an impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiffs' PII right in the hands of criminals.

32. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries. Today, Plaintiff has a continuing interest in ensuring that her

PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Andrew Gilsey

33. Plaintiff Andrew Gilsey is and at all times relevant was, a resident of Greene and a citizen of the state of New York.

34. Plaintiff Gilsey is a consumer who had a cellular phone account with Defendant for approximately seven years until 2020.

35. As a condition of receiving services from Defendant, Plaintiff Gilsey was required to provide his PII, including her full name, address, phone number, date of birth, and Social Security Number, to Defendant. Defendant used that PII to facilitate its provision of services and operate its business.

36. Plaintiff provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained Plaintiffs' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

37. Plaintiff received a Notice of Data Breach in April 2024.

38. On information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

39. Plaintiff Gilsey fears for his personal financial security and worries about what information was exposed in the Data Breach. Indeed, Plaintiff recently suffered fraudulent charges on a debit card and was forced to expend time and effort to address those fraudulent charges.

40. Plaintiff suffered imminent an impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiffs' PII right in the hands of criminals.

41. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries. Today, Plaintiff has a continuing interest in ensuring that his

PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Tina Young

42. Plaintiff Tina Young is and at all times relevant was, a resident of Lancaster and a citizen of the commonwealth of Pennsylvania.

43. Plaintiff Young is a consumer who has had a cellular phone account with Defendant for approximately two years. Prior to that, Plaintiff Young had a DirectTV account with AT&T for approximately four years between 2019 and 2023.

44. As a condition of receiving services from Defendant, Plaintiff Young was required to provide her PII, including her full name, address, phone number, date of birth, and Social Security Number, to Defendant. Defendant used that PII to facilitate its provision of services and operate its business.

45. Plaintiff provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiffs' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

46. Plaintiff received a Notice of Data Breach dated April 25, 2024.

47. Thus, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

48. Plaintiff Young fears for her personal financial security and worries about what information was exposed in the Data Breach.

49. Plaintiff suffered imminent an impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiffs' PII right in the hands of criminals.

50. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries. Today, Plaintiff has a continuing interest in ensuring that her

PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Anna Palafox

51. Plaintiff Anna Palafox is and at all times relevant was, a resident of Chicago and a citizen of the state of Illinois.

52. Plaintiff Palafox is a consumer who has had a cellular phone account with Defendant for approximately a year between 2019 and 2020.

53. As a condition of receiving services from Defendant, Plaintiff Palafox was required to provide her PII, including her full name, address, phone number, date of birth, and Social Security Number, to Defendant. Defendant used that PII to facilitate its provision of services and operate its business.

54. Plaintiff provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiffs' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

55. Plaintiff received a Notice of Data Breach in April 2024.

56. Thus, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

57. Plaintiff Palafox fears for her personal financial security and worries about what information was exposed in the Data Breach.

58. Plaintiff suffered imminent an impending injury arising from the substantially increased risk of fraud, misuse, and identity theft. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries. Today, Plaintiff has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Tina Salinas

59. Plaintiff Tina Salinas is and at all times relevant was, a resident of Lamarque and a citizen of the state of Texas.

60. Plaintiff Salinas is a consumer who has cellular phone service, internet service, and television services with Defendant for a long period of time, some accounts existing prior to the purchase of AT&T by Southwestern Bell.

61. As a condition of receiving services from Defendant, Plaintiff Salinas was required to provide her PII, including her full name, address, phone number, date of birth, and Social Security Number, to Defendant. Defendant used that PII to facilitate its provision of services and operate its business.

62. Plaintiff provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiffs' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

63. Plaintiff received a Notice of Data Breach dated April 2, 2024.

64. Thus, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

65. Plaintiff Salinas fears for her personal financial security and worries about what information was exposed in the Data Breach.

66. Plaintiff suffered imminent an impending injury arising from the substantially increased risk of fraud, misuse, and identity theft. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries. Today, Plaintiff has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Latoya Pettus

67. Plaintiff Latoya Pettus is and at all times relevant was, a resident of North Little Rock and a citizen of the state of Arkansas.

68. Plaintiff Pettus is a consumer who has cellular phone service through Defendant since approximately 2013.

69. As a condition of receiving services from Defendant, Plaintiff Pettus was required to provide her PII, including her full name, address, phone number, date of birth, and Social Security Number, to Defendant. Defendant used that PII to facilitate its provision of services and operate its business.

70. Plaintiff provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiffs' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

71. Plaintiff received a Notice of Data Breach on in April 2024.

72. Thus, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

73. Plaintiff Pettus fears for her personal financial security and worries about what information was exposed in the Data Breach.

74. Plaintiff suffered imminent an impending injury arising from the substantially increased risk of fraud, misuse, and identity theft. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries. Today, Plaintiff has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Defendant AT&T, Inc.

75. Defendant AT&T, Inc. is a Delaware corporation with its principal place of business located at 208 South Akard Street in Dallas, Texas. Defendant can be served through their registered agent CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. AT&T is a publicly

traded company organized and operated for the profit and financial benefit of its shareholders. In 2023, AT&T had annual revenue of over $122.4 billion, with net income over $14.1 billion. AT&T has often attempted to distinguish itself from its competitors by promoting its purportedly unique customer experience. For example, on its website, AT&T states that: "As one of the largest advertisers in the U.S., AT&T strives to create marketing messages that accurately represent society as well as our products and services."[9]

JURISDICTION AND VENUE

76. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). This lawsuit is a class action with an amount in controversy over $5 million, involving over 100 proposed class members, some of whom are from a different state than Defendant.

77. This Court may exercise personal jurisdiction over Defendant because Defendant is registered to do business and has its principal place of business in this district.

78. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background

AT&T Expends Billions to Transform Itself into a Modern Media Company While Placing Profits Ahead of Providing Adequate Cyber-Security

79. For several years prior to the Data Breach, AT&T invested significantly in an expansion of its platform and footprint to transform itself into a modern media company. In a February 3, 2020 letter to AT&T investors executed by then CEO and Board Chairman Randall Stephenson, included in the Company's 2019 Annual Report in February 2020 ("2019 Annual

[9] https://about.att.com/csr/home/reporting/issue-brief/responsible-marketing.html (Last visited August 2, 2024)

Report"), it was reported that "over the past several years, we've made a series of strategic investments to drive a major transformation of our Company."

80. Chairman and CEO Stephenson further reported on February 3, 2020, that, among other things, "we're now in full execution mode and moving forward as a modern media company… at a time when … content and connectivity trends have arrived sooner than many anticipated." AT&T further reported that its investments in building out its connectivity infrastructure and platform exceeded $30 Billion, boasting that "AT&T has the best and fastest wireless network in the United States," and that "by year end 2019, we had launched 5G to 50 million people, and we expect to have nationwide coverage in the second quarter of 2020." AT&T projected that in 2020 its gross capital investment would approximate $20 billion.

81. In the 2019 Annual Report, AT&T acknowledged facing a significant risk of Cyberattacks, stating that:

> Cyberattacks . . . or other breaches of network or IT security that affect our networks, including software and switches, microwave links, third-party-owned local and long-distance networks on which we rely, our cell sites or other equipment, our satellites, our customer account support and information systems, or employee and business records could have a material adverse effect on our operations.

82. In the 2019 Annual Report, the Company went so far as to acknowledge being the target of cyberattacks, even while it downplayed their existence, stating that:

> While we have been subject to security incidents or cyberattacks, these did not result in a material adverse effect on our operations. However, as such attacks continue to increase in scope and frequency, we may be unable to prevent a significant attack in the future. Our ability to maintain and upgrade our video programming also depends on our ability to successfully deploy and operate video satellites. ***Our inability to*** deploy or operate our networks or customer support systems or ***protect sensitive personal information of customers*** or valuable technical and marketing information could result in significant expenses, potential legal liability, a loss of current or future customers and reputation damage, any of which could have a material adverse effect on our operations and financial condition.

(emphasis added).

83. On February 25, 2021, AT&T issued its 2020 Annual Report (the "2020 Annual Report"), wherein it repeated, *verbatim*, the warnings included in the 2019 Annual Report.

84. On February 17, 2022, AT&T's new Chief Executive Officer, John Stankey, in a letter to shareholders contained in the Company's 2021 Annual Report, (the "2021 Annual Report"), noted that in the wake of the COVID pandemic, "the internet has become a lifeline for many – a connection to

friends, family, work, commerce, education, health, entertainment, and more," adding that "it's no surprise that during this pandemic, AT&T experienced its largest annual increase in data traffic in 2021."

85. CEO Stankey's February 17, 2022 letter reported that AT&T was in a "the dawn of a new age of connectivity," and commented that the new age was "powered by the widespread growing availability of 5G and fiber, … defined by greater ubiquity, reliability, **security**, capacity and speed." (Emphasis provided). According to AT&T's 2021 Annual Report, and as confirmed in CEO Stankey's letter, as of that time the Company had more than 255 million people with nationwide 5G service on a wireless network which CEO Stankey represented was "recognized as being both the best and most reliable," and with respect to HBO Max, the Company grew it to "nearly 74 million global HBO Max and HBO's subscribers."

86. In a section of the CEO's February 17, 2022 letter titled "Effective and Efficient in Everything We Do: increasing profitability, reinvesting for growth," it was stated that "our cost savings have been reinvested into our growth areas, driving and improve customer experience, lower turn and healthy growth." A section of the 2021 Annual Report entitled "Operating Environment and Trends of the Business," exemplifying AT&T's concern about cost and expenses amid the enlargement of its customer base, stated in pertinent part:

> **2022 Expense Trends** We expect the spending required to support growth initiatives, primarily our continued deployment of fiber and 5G, including 3G shutdown costs in the first quarter of 2022, as well as continued investment into the HBO Max platform, to pressure expense trends in 2022 …The software benefits of our 5G wireless technology should result in a more efficient use of capital and lower network-related expenses in the coming years.
>
> ***
>
> We continue to transform our operations to be more efficient and effective, reinvesting savings into growth areas of the business. We are restructuring businesses, sunsetting legacy networks, improving customer service and ordering functions through digital transformation, sizing our support costs and staffing with current activity levels, and reassessing overall benefit costs. Cost savings and asset sales align with our focus on debt reduction.

87. In a February 13, 2023 letter to shareholders executed by CEO Stankey and filed with the Company's 2022 Annual Report ("2022 Annual Report"), it was reported that the Company attracted "nearly 2.9 million post-paid phone net additions in 2022" respecting U.S. Wireless, further commenting that "the strength of our wireless network played a large role in our success," adding regarding Wireless that the Company was able to "reach more than 150 million people, more than double our original year-end coverage target," while noting that "we expect to hit 200 million people by the end of 2023." It was reported that AT&T "delivered strong full-year results in AT&T Fiber as well," with 2022 marking its "fifth straight year with one million or more net additions, raising our AT&T Fiber subscriber based to more than 7 million" making the Company "a leader in bringing Fiber to homes and closing the year with an ability to serve more than 19 million consumer locations" and "more than 3 million business locations, … on track to reach our previously announced goal of 30 million plus total locations, including consumer and business, by the end of 2025."

88. In a section of the 2022 Annual Report entitled "Operating Environment and Trends of the Business," subpart captioned "2023 Expense Trends," AT&T again focused attention on cost savings stating in pertinent part:

> **2023 Expense Trends** We expect the spending required to support growth initiatives, primarily our continued deployment of fiber and 5G to pressure expense trends in 2023. To the extent customers further upgrade their handsets in 2023, the expenses associated with those device sales are expected to contribute to higher costs. During 2023, we will also continue to prioritize efficiency, led by our cost transformation initiative. … We continue to transform our operations to be more efficient and effective. We are restructuring businesses, sunsetting legacy networks, improving customer service and ordering functions through digital transformation, sizing our support costs and staffing with current activity levels, and reassessing overall benefit costs. Cost savings and asset sales align with our focus on debt reduction.

89. In a February 23, 2024 letter to shareholders executed by CEO John Stankey that was included in the Company's 2023 Annual Report ("2023 Annual Report"), AT&T's CEO remarked that "2023 was another year of strong, consistent performance that bolster's confidence in our strategy to be the best connectivity provider through 5G and Fiber," adding that "[i]n 2023, we delivered on our long-

term growth strategy in three important ways: we grew durable 5G and Fiber relationships; with a continued focus on effective and efficient operations, we achieved our three year, 6 billion plus run-rate cost transformation target ahead of schedule and our making progress on an incremental $2 billion plus in targeted savings by mid-2026; and [o]ur deliberate capital allocation strategy supporting another year of historic 5G and Fiber investment levels …"

90. It was further noted in the CEO's letter that "[o]ver the past three years, AT&T has consistently communicated and executed an investment-led strategy built on one fundamental principle: [c]ustomers increasingly value converged services," adding "[t]hey want a single provider who can support their connectivity needs both at home and on the go, delivering a seamless experience that allows them to connect to what they love from anywhere."

91. AT&T further reported that it was North America's largest wireless network and the nation's largest and fastest growing Fiber network stating, "no company is better suited to answer the call for widespread connectivity than AT&T." AT&T represented that "the size and quality of our network has never been better," while noting with respect to wireless that "[W]e achieved our coverage target, reaching more than 210 million people with our nationwide mid-band 5G network to offer faster speeds and enhance the experience on the nation's most reliable 5G network." With respect to "Fiber" it was noted that the Company "marked another year" in 2023 of "consistent leadership and fiber deployment" adding one million or more new Fiber customers for the sixth straight year.

92. CEO Stankey's letter included in AT&T's 2023 Annual Report provided an entirely updated and new section entitled "Acting Responsibly," within which he stated "[W]e are one of America's critical infrastructure providers, and with that brings a **responsibility** to be a leader in helping to connect every American to the internet and to build world-class wireless and broadband infrastructure," adding "[A]s a nation, we have dedicated substantial private and public resources to building an excellent foundation for future of the fast, reliable and affordable connectivity." (Emphasis provided).

93. All the while, as it invested to expand, Defendant remained especially conscious of reducing operating costs that could materially impact the bottom line. As reflected in the 2023 Annual

Report's statement of "Risk Factors," the Company voiced concern respecting inflationary pressures on costs and labor and distribution costs, its financial condition, and its results of operations as a provider of telecommunications and technology services. In a sub-section included in its discussion of "Risk Factors" entitled "Cyber-attacks Impacting our Networks or Systems May Have a Material Adverse Effect on our Operations," AT&T's 2023 Annual Report represented that "[W]hile, to date, we have not been subject to cyberattacks that individually or in the aggregate, have been material to our operations or financial condition, the preventive actions we take to reduce the risk associated with cyberattacks may be insufficient to repel or mitigate the effects of a major cyberattack in the future." Upon information and belief, AT&T's so-called "preventive" actions were woefully inadequate and insufficient.

94. Defendant's clear awareness of the need for cyber-security is further reflected in its 2023 Annual Report under a new section entitled, "Item 1C. **CYBER SECURITY**," and a subpart entitled "Governance," in which AT&T discussed Board and Audit Committee oversight, representing that its Board of Directors delegated to the Audit Committee the oversight responsibility to review and discuss with management the Company's privacy and data security, including cyber security, risk exposures, policies and practices, the steps management taken to detect, monitor, and control such risks, and the potential impact of those exposures on its financial results, operations and reputation. It was further disclosed that the "full Board and Audit Committee regularly receives reports and presentations on privacy and data security, which addressed relevant cyber security issues and risks and span a wide range of topics." AT&T represented that these "reports and presentations are provided by officers with responsibility for privacy and data security who include our Chief Information Security Officer ("CISO"), Chief Technology Officer ("CTO"), and AT&T's Legal team." Any such reporting would have provided clear knowledge that AT&T's cyber-security was deficient, exposing tens of millions of consumers to the theft of their PII as the ever expanding Company placed profits ahead of consumers' cyber-security and privacy.

95. AT&T falsely represented that the Company maintained a network and information security program "reasonably designed to protect our information, and that of our customers, from unauthorized risk to their confidentiality, integrity, or availability, … [A]ssessing, verifying, and

managing risk from cyber security threats, including third-party risk from vendors and suppliers," and a "program" … "designed to identify and respond to security incidents and threats in a timely manner to minimize the loss or compromise of information assets and to facilitate incident resolution."

96. The 2023 Annual Report further represented, in pertinent part, as follows:

> **CYBERSECURITY**
>
> **Risk Management and Strategy**
> We maintain a network and information security program that is reasonably designed to protect our information, and that of our customers, from unauthorized risks to their confidentiality, integrity, or availability…
>
> **Impact of Cybersecurity Risk**
>
> In 2023, we did not identify and were not aware of any cybersecurity breaches that we believe have materially affected or are reasonably likely to materially affect our business strategy, results of operations, or financial condition…

97. Defendant was well aware of the possibility of a major cyber-attack, no doubt because it was also aware, upon information and belief, that it had not implemented sufficient or adequate cyber security to protect its consumers as it greatly expanded its network and footprint, which exacerbated such cyber-security inadequacies.

98. AT&T's cyber-security was woefully deficient, inadequate, and insufficient. AT&T failed and continues to fail to adopt, implement, and maintain reasonable and adequate security measures that are absolutely critical and necessary to protect its customers and consumers from unauthorized access and/or exploitation or exfiltration of their PII. Plaintiffs are informed and believe and thereupon allege that the Company has consistently failed to encrypt the data and has consistently failed to implement necessary safeguards to protect against the ability of cyber thieves to access its systems and information systems and networks, exploiting seams or defects therein, to unlawfully profit thereby.

99. The implementation of a CSIO or report of "cyber security" protocols or processes that only for the first time were noted in the Company's 2023 Annual Report amounted to "too little, too late." The Company was spending billions on expansion in order to increase revenue and profitability, while

continuously and consciously failing spend required monies needed to build and maintain a proper, adequate cyber security to protect unauthorized access to PII. Defendant failed to rectify this knowing problem that AT&T's rapid expansion of connectivity and its footprint in pursuit of becoming a modern mobile and media leader, spending billions and billions over a number of years, while failing to simultaneously address the need to also expend sufficient monies to protect consumers from unauthorized access to their PII resulting from cyber-attacks that AT&T knew was a significant risk and, upon information and belief, also knew was a risk that had been exacerbated by their rapid expansion and buildout.

100. AT&T placed profits ahead of cyber security protection, exposing unwitting customers to the invasion of their privacy and theft of their Private Information and data, which it knew, at all times material, was at risk of unauthorized access by cyber thieves who saw the mobile and telecommunications industry, and especially AT&T, as a prime target ripe for attack.

AT&T is Required to Protect Consumers' Privacy

101. AT&T provides telecommunications, internet, or other services to more than 100 million U.S. consumers.[10] It is self-described as "the future of connectivity." *Id.*

102. AT&T collects, maintains and profits from the PII of tens of millions of prospective and current customers, profits from the PII regardless of whether a potential customer eventually selects AT&T as his or her wireless carrier. AT&T also maintains the PII for an indefinite period of time.

103. Since at least 2018, AT&T has maintained privacy policies by which it assured consumers that it would protect their PII.

104. For example, As of January 31, 2019, AT&T Communications' privacy policy (the "2019 Privacy Policy"), published on AT&T's website and in place since July 21, 2018, provided, *inter alia*, that:

[10] https://investors.att.com/investor-profile#:~:text=AT%26T%20Communications%20provides%20more%20than,expansion%20and%20wireless%20network%20enhancements, last visited August 2, 2024.

- We will protect your privacy and keep your personal information safe. We use encryption and other security safeguards to protect customer data.[11]

The 2019 Privacy Policy further provided that:

- We keep your Personal Information in our business records while you are a customer, or until it is no longer needed for business, tax or legal purposes.
- We will keep your information safe using encryption or other appropriate security controls.[12]

105. In the current version of its privacy policy (the "Privacy Policy"), AT&T represents that it will maintain the security and privacy of customers' personal information. For instance, AT&T states the following in its Privacy Policy:

> We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.[13]

106. The Privacy Policy also provides that Defendant collects a broad range of information on its customers including, *inter alia*:

- Name, postal address, email address, account name, Social Security number, driver's license number, passport number, taxpayer identification number, IP address, device IDs;
- Age, age range, date of birth, gender, preferred language, marital status;
- Biometric information such as Fingerprint, voiceprint, or scan of face geometry, that is used to identify a specific individual;
- Education information such as Degree(s), actual or inferred level of education;

---

11 https://web.archive.org/web/20190131235126/http://about.att.com/sites/privacy_policy, last visited August 2, 2024.

12 *Id.*

13 https://about.att.com/privacy/privacy-notice.html, last visited August 2, 2024.

- Professional or employment related information such as Current or past employment; history, licenses and professional membership.[14]

107. As of 2023, AT&T's "Customer Data Privacy" policy has stated: "Data helps us create more reliable products and services, improve security and detect fraud, and provide customers with customized offers. Customers also count on AT&T to **protect** their **information** and **respect** their **privacy**. We take this **responsibility** seriously and work hard to maintain customers' trust." (Hereinafter "Privacy Policy").[15] (Emphasis provided)

108. This Privacy Policy states that it applies to "information generated when you use or subscribe to AT&T products, services, apps, websites or networks to which this Policy is linked." Information, in this context, is about "you and how you're using our Products or Services along with information about your devices and equipment." This includes "data like your performance information, along with web browsing, location and video viewing information." It further states that the Notice applies to "anyone who uses our Products or Services under your account"[16]

109. This Privacy Policy assured customers that AT&T aggregates data before sharing it, "which means that we group the information so that it does not identify consumers personally, and we require anyone who receives this data to agree they will only use it for aggregate insights, won't attempt to identify any person or device using this information, and will handle it in a secure manner, consistent with this Policy."[17]

110. The California Privacy Rights section of the Privacy Policy, included for purposes of complying with the California Consumer Protection Act ("CCPA") stated, as of 2023, that "[w]e don't knowingly allow other parties to collect personally identifiable information about your online activities

14 https://about.att.com/privacy/privacy-notice/state-disclosures.html#we-collect, last visited August 2, 2024.

15 https://about.att.com/privacy/full_privacy_policy.html (Last visited August 2, 2024).

16 *Id.*

17 *Id.*

over time and across non-AT&T company websites for their own use when you use our websites and services, unless we have your consent."[18]

111. AT&T assured consumers that it would only share data under certain enumerated circumstances, which include: "with your consent or at your direction," "with the account holder," "between AT&T brands and companies," "to provide benefits," "to our service providers," "to other third parties for uses described in this notice or for purposes you have requested," "for identity verification and fraud prevention services," "caller ID providers," "in a business transfer or transaction" which is specified as a "corporate business transaction like an acquisition, divestiture, sale of company assets," and "for legal process and protection." None of the enumerated circumstances involve sharing Plaintiff's or the Class Members' PII with a criminal hacker. AT&T pledges that consumers' PII is secure, stating that: (i) personal data will be disclosed only "with your consent, which we may get in writing, online, or orally," and (ii) AT&T uses "administrative, technical, contractual, and physical safeguards designed to protect your data." As discussed herein, AT&T failed to comply with these promises to protect Consumers' Plaintiffs' and Class Members' PII.

112. To further comfort consumers, AT&T "we're working hard to earn a place in your heart. A big part of that is maintaining your privacy. We believe you deserve transparency, education, choice, protection, and simplicity." - assurances that are far from the reality of AT&T's cyber-security and have proven untrue given the millions of consumers affected by AT&T's breach of trust and failure to protect their PII.

A. *The Data Breach*

113. Defendant AT&T, Inc., is a Dallas, Texas-based telecommunications provider that provides, *inter alia*, cellular wireless services and internet services to consumers throughout the United States.

[18] *Id.*

114. On or about March 30, 2024, AT&T posted a notice on its website stating that "a number of AT&T passcodes have been compromised."[19] The notice further stated that "we will be communicating with current and former account holders with compromised sensitive personal information" but provided no specifics about the "sensitive personal information" involved in the Data Breach.[20] AT&T confirmed that, approximately two weeks prior to its announcement, the "data set," relating to 7.6 million current AT&T customers and approximately 65.4 million former account holders, had been released on the dark web.[21,22,23] AT&T further acknowledged that this "data set" included critical PII such as names, Social Security numbers, email addresses, mailing addresses, phone numbers, and birth dates.

115. News reports further indicate that this "data set" appears to relate to a data breach (the "Data Breach") that occurred in 2021, but was never acknowledged or remedied by AT&T.[24] At least one news outlet reports that AT&T disputes any connection to a 2021 Data Breach, however, the Company has identified neither who is responsible for the Data Breach nor when it occurred.[25] Notably, in 2021, when data purportedly from this 2021 breach surfaced, AT&T denied that its customer data security had been breached.[26] Similarly, on March 22, 2024, when *TechCrunch* initially reported on the release of AT&T data on the dark web, AT&T stated, "We have no indications of a compromise of our

[19] *See* https://www.att.com/support/article/my-account/000101995?bypasscache=1, last visited August 2, 2024.

[20] *Id.*

[21] https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html, last visited August 2, 2024.

[22] *See https://fortune.com/2024/03/31/att-data-breach-over-70-million-dark-web/*, last visited August 2, 2024.

[23] https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web, last visited August 2, 2024.

[24] https://techcrunch.com/2024/03/22/att-customers-data-leak-online/?guccounter=1 , last visited August 2, 2024.

[25] https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web, last visited August 2, 2024.

[26] https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web, last visited August 2, 2024.

systems. We determined in 2021 that the information offered on this online forum did not appear to have come from our systems. This appears to be the same dataset that has been recycled several times on this forum."[27]

116. AT&T's failure to protect the PII of current and former customers, and its failure to timely disclose the Data Breach, has left tens of millions of Class Members at heightened risk of financial fraud and identity theft.

B. ***AT&T's History of Ongoing and Significant Data Breaches***

117. AT&T has experienced an ongoing series of cyber-security incidents over the years. These breaches are a result of its ongoing flawed and inadequate cyber-security.

118. A 168-day data breach took place at an AT&T call center in Mexico between November 2013 and April 2014. During this period, three call center employees were paid by third parties to obtain customer information — specifically, names and at least the last four digits of customers' Social Security numbers. The three call center employees accessed more than 68,000 accounts without customer authorization. The FCC's Enforcement Bureau determined that those data breaches occurred when employees at call centers used by AT&T in Mexico, Colombia, and the Philippines accessed customer records without authorization. These employees then provided the information to unauthorized third parties who appear to have been trafficking in stolen cell phones or secondary market phones that they wanted to unlock. [28]

119. In 2015, AT&T agreed, in cooperation with the Federal Communications Commission, to pay $25 Million to settle three consumer privacy investigations.[29]

120. According to a reliable confidential source ("CW1"), possessing first-hand knowledge, in mid-2022, AT&T's CTO was warned by CW1 of a significant risk relating to the use of third-party contractors. CW1 had an extensive work history with AT&T as a senior network architect and as a task

---

27 *Id.*

28 https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches-0

29 *Id.*

lead providing network support. In the course of working in those roles, CW1 learned that AT&T allowed third party contractors access to certain of its databases containing customer information for the purpose of troubleshooting network issues. CW1 found this especially concerning because this access was provided to foreign contractors. As a result CW1 was concerned that AT&T's lax data access policies left it vulnerable to cyber-attacks through its third-party vendors, yet, it did nothing to contain the situation or neutralize the clear and existing risk.

121. In August 2021, a hacking group had claimed that it was selling data relating to millions of AT&T customers: "AT&T Database + 70M (SSN/DOB)." It published a small sample of the leaked data at that time. Plaintiffs are informed and believe and thereupon allege that this criminal hacking group is Shiny Hunters, which informed AT&T in August 2021 that the customer PII from their cyber-theft would be sold online.[30] The data that the cyber thieves intended to auction online was observed by *Hackread*, a technology site, as including full names, addresses, zipcodes, dates of birth, email addresses, and Social Security numbers. Although it was aware of the auction of this PII, AT&T denied that any data came from its servers.

122. The Data Breach occurred as a consequence of AT&T's inadequate cyber-security systems. As AT&T has now conceded and disclosed, the Data Breach involved the PII of more than 70 million current and former customers, after which cyber thieves leaked their information on the dark web. According to AT&T, 7.6 million current account holders and 65.4 million former account holders were impacted by the Data Breach. The information that was secured includes some of the most significant personal information upon which data thieves can create false identities or otherwise monetize the sale of such information on the dark web: Social Security Numbers, full names, email and mailing addresses, phone numbers, dates of birth, AT&T account numbers and passcodes. Demonstrating the utter failure

[30] Wagas, AT&T breach? ShinyHunters selling AT&T database with 70 million SSN, HACKREAD (Aug. 20, 2021), http://www.hackread.com/att-breach-shinghunders-database-selling-70-million-ssn. (Last visited August 2, 2024).

to maintain adequate cyber-security, the Company has acknowledged that "the data set appears to be from 2019 or earlier."[31]

123. According to an article appearing in "TechCrunch" on March 22, 2024, an analysis of the more fully leaked data set pointed to AT&T customer data being authentic, and AT&T customers ultimately confirmed that their leaked customer data was accurate.[32] TechCrunch reported "but AT&T still hasn't said how its customers data spilled online."[33] According to Troy Hunt, the full leaked dataset contained 73 million leaked records, with 49 million unique email addresses, 44 million Social Security Numbers and customers' birth dates.[34]

124. AT&T again suffered a massive data breach in and or around January 2023, compromising the sensitive personal information of approximately 9 million consumers in the United States.

125. Clearly, AT&T has still not adequately addressed cyber-security despite these prior experiences. Even as recently as July 12, 2024, yet another data breach has been disclosed. In an article appearing in CNN Business by Matt Egan and Sean Lyngaas, dated July 22, 2024, entitled "Nearly All AT&T Sale Customers' Call and Text Records Exposed in a Massive Data Breach," it was reported that call and text message records from mid-to-late 2022 of tens of millions of AT&T cell phone customers and many non-AT&T customers were exposed in a data breach revealed by AT&T.[35] According to AT&T, "the compromised data includes the telephone numbers of 'nearly all' of its cellular customers and the customers of wireless providers that use its network between May 1, 2022 and October 31,

---

[31] https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web#:~:text=Millions%20of%20customers%27%20data%20found,in%20latest%20AT%26T%20data%20breach&text=Richard%20Drew%2FAP-,An%20AT%26T%20store%20in%20New%20York.,to%207.6%20million%20current%20customers, last visited August 2, 2024.

[32] https://techcrunch.com/2024/03/22/att-customers-data-leak-online/?guccounter=1, last visited August 2, 2024.

[33] *Id*.

[34] *Id*.

[35] https://www.cnn.com/2024/07/12/business/att-customers-massive-breach/index.html, last visited August 2, 2024.

2022."[36] Stolen logs reportedly contains a record of every number AT&T customers called or texted – including customers of other wireless networks, the number of times they interacted, and the call duration. While AT&T maintains that the stolen data did not include the contents of calls and text messages, nor the time of the communications, this latest data breach and privacy intrusion merely underscores the fact that AT&T has failed to maintain adequate cyber-security and that its failure is conscious, deliberate, and unacceptable.

126. According to the July 12, 2024, CNN article, it was reported by the Federal Communications Commission on social media platform X that "[W]e have an ongoing investigation into the AT&T breach and we're coordinating with our law enforcement partners."[37]

127. The latest incident had "no connection in any way" to the Data Breach of disclosed in March 2024, according to AT&T, which involves personal information, including Social Security Numbers, on 73 million current and former customers that was released on to the dark web. But the most recent data breach revealed in July 2024, involved approximately 110 million wireless subscribers as of the end of 2022, and included AT&T landline customers who interacted with those cell numbers.

128. AT&T has reported that it learned that a "threat actor claimed to have unlawfully accessed and copied AT&T call logs" on April 19, 2024, after which an investigation had determined that hackers had exfiltrated files between April 14 and April 25, 2024.

129. AT&T maintains that the U.S. Department of Justice determined in May 2024 and in June, 2024, that a delay in public disclosure of the April 2024 breach was warranted.[38]

130. This most recent cyber incident is "very concerning" according to Sanaz Yashar, co-founder and CEO of cyber-security firm Zafran, because threat actors can correlate the sale of ID data with other information readily available to pinpoint where someone works – including at sensitive

[36] *Id*.

[37] https://www.cnn.com/2024/07/12/business/att-customers-massive-breach/index.html, last visited August 2, 2024.

[38] *Id*.

locations like the White House and Pentagon.[39] Justin Sharman, founder of Global Cyber Strategies, a consultancy, has remarked that "metadata about who's communicating with who, at massive scale, enables someone to map connections between people – think journalist and sources, intelligence officers and their contacts, married people, those with whom they are having an affair." *Id*. Jason Hogg, a former FBI Special Agent has commented that the sale cite data is "quite significant because it could allow bad actors to determine certain customers' geolocation, which could be used to make the social engineering attacks more believable."[40]

131. According to AT&T, the most recent cyber-attack was a consequence of an illegal download from its workspace on Snowflake, a third-party cloud platform.[41]

132. AT&T was clearly aware at all times material to the March 2024 Data Breach and at all other relevant times of its data security failures. Prior and subsequent breaches powerfully demonstrate that Plaintiffs' PII, which remains in AT&T's possession, is simply not safe.

C. *AT&T is Well Aware of the Threat of Cyber Theft and Exfiltration in the Telecommunications Industry*

133. As a condition of its relationships with its customers, including Plaintiffs and Class Members, Defendant required that they entrust it with highly sensitive and confidential PII. Defendant, in turn, collected that information and assured consumers that it was acting to protect that PII and to prevent its disclosure.

134. Plaintiffs and Class Members, who were required to provide their PII, did so with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access and disclosure.

135. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on Defendant to keep their PII confidential and securely

[39] *Id.*

[40] https://www.cnn.com/2024/07/12/business/att-customers-massive-breach/index.html, last visited August 2, 2024.

[41] *Id.*

maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

136. Defendant could have prevented the Data Breach by assuring that the PII at issue was properly secured.

137. Defendant's overt negligence in safeguarding Plaintiffs' and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as a business operating in the telecommunications space, Defendant was on notice that companies in that industry are targets for data breaches, especially in light of the massive 2021 data breach at competitor T-Mobile.

138. PII, including names and social security numbers are uniquely valuable to hackers. With these pieces of information, criminals can open new financial accounts in Class Members' names, take loans in their names, use their names to obtain medical services, obtain government benefits and/or identification, file fraudulent tax returns in order to get refunds to which they are not even entitled, and numerous other assorted acts of thievery and fraud.

139. In 2023, cyber intelligence firm Cyble noted that U.S. telecommunications companies are a lucrative target for hackers. Cyble observed that many of the recent data breaches could be attributed to third-party vendors, and further commented that "[T]hese third-party breaches can lead to a larger scale supply-chain attacks and a greater number of impacted users and entities globally."[42]

140. Social Security numbers are among the most sensitive kind of personal information and the hardest to rehabilitate if it is misused or misappropriated. An individual cannot easily obtain a new Social Security number. Doing so, requires the completion of significant paperwork and provision of evidence of actual misuse. In other words, preventive action to guard against potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.

[42] https://cyble.com/blog/u-s-telecommunications-companies-targeted-consumers-hit-hardest/, last visited August 2, 2024.

141. A new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

142. For this reason, hackers prey on companies that collect and maintain sensitive financial information, including telecommunications companies. Companies, like AT&T, have been aware of this, and the need to take adequate measures to secure their systems and customer information, for a number of years.

143. In 2021, 1,862 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, an increase of 68% over 2020 and a 23% increase over the previous all-time high. These data breaches exposed the sensitive data of approximately 294 million people. Id. Hackers are increasingly targeting highly sensitive PII, including social security numbers and, in 2021, approximately 1,136 data breaches exposed social security numbers.

144. Companies, like Defendant AT&T, are well aware of the risk that data breaches pose to consumers, especially because both the size of their customer base and the fact that the PII that they collect and maintain is profoundly valuable to hackers. Indeed, Federal Reserve Chairman Jerome Powell has referred to cyber-attacks as the number one threat to the global financial system.

145. It can be inferred from the Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs' and Class Members' PII.

146. Upon information and belief, prior to the Data Breach, Defendant was aware of its security failures but failed to correct them or to disclose them to the public, including Plaintiffs and Class Members.

147. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendant knew or should have known that it did not make such actions and failed to implement adequate data security practices.

148. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the PII of Plaintiffs and Class Members; and without the Court's intervention via injunctive relief, Representative Plaintiffs' and Class Members' PII remains at risk of subsequent data breaches.

149. Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and financial information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII financial information of Plaintiffs and Class Members.

150. Defendant owed a duty to Plaintiffs and Class Members to ensure that the PII it collected and was responsible for was adequately secured and protected.

151. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

152. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach that impacted the PII it collected and was responsible for in a timely manner.

153. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

154. Defendant owed a duty to Plaintiffs and Class Members to disclose if its data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

155. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

156. Defendant owed a duty to Plaintiffs and Class Members to mitigate the harm suffered by the Representative Plaintiffs' and Class Members' as a result of the Data Breach.

157. As a direct and proximate result of Defendant's reckless and negligent actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, and Defendant's failure to properly and timely notify Plaintiffs and Class Members, Plaintiffs and Class Members are more susceptible to identity theft and have experienced, will continue to experience and will face an increased risk of experiencing the following injuries, *inter alia*:

a. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;
b. money and time lost as a result of fraudulent access to and use of their financial accounts;
c. loss of use of and access to their financial accounts and/or credit;
d. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
e. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;
f. lowered credit scores resulting from credit inquiries following fraudulent activities;
g. money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;
h. costs and lost time obtaining credit reports in order to monitor their credit records;
i. anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;
j. costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

k. money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;

l. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;

m. loss of the opportunity to control how their personal information is used; and

n. continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Defendant fails to undertake appropriate, legally required steps to protect the personal information in its possession.

158. Identity theft and also exacts an emotional and physical toll on victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.
- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and

- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[43]

D. *AT&T's Inadequate Data Security Violated the FTC Act and the FCA and Failed to Adhere to Regulatory Guidelines and Industry – Standard Cyber Security Practices*

159. Pursuant to the Federal Trade Commission Act of 1915 ("FCTA"), AT&T was required to undertake reasonable and appropriate measures to protect the PII entrusted to it from unauthorized disclosure. Similarly, pursuant to the Federal Communications Act ("FCA"), common carriers, such as AT&T, are required to protect the consumer PII entrusted to it.

160. The Federal Trade Commission ("FTC") has adopted and published guidelines establishing reasonable and appropriate data security measures for businesses such as AT&T. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

161. The FTC has also published guidance titled, "Protecting Personal Information: A Guide for Business," which addresses steps that businesses should take to protect sensitive consumer data, including noting that: "[i]f you don't have a legitimate business need for sensitive personally identifying information, don't keep it."[44], Despite this guidance, AT&T appears to have kept a large amount of PII belonging to consumers who were no longer AT&T's customers. In addition, the FTC guide for business provides guidelines for maintaining network and data security, user authentication, breach detection, and

[43] *Identity Theft: The Aftermath 2017*, ITRC, https://www.idtheftcenter.org/wpcontent/uploads/images/page-docs/Aftermath_2017.pdf (last visited August 2, 2024).

[44] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business, last visited August 2, 2024

other critical security best practices.[45] AT&T's failure to follow FTC guidelines, including, but not limited to, maintaining data on former customers, violated the guidelines. In addition, by its failure to adopt and maintain reasonable and adequate data security processes, AT&T engaged in unfair acts or practices within the meaning of the FTC Act.

162. Plaintiffs are informed and believe and on that basis allege that AT&T's ongoing data security failure arising from an apparent conscious decision not to expend funds necessary to upgrade, provide or implement adequate cybersecurity measures so that consumers are adequately protected from unauthorized access of their PII, flies in the face of and fails to comply with, state and federal laws and requirements, as well as industry standards governing the protection of PII.

163. AT&T failed to comply with critically important Federal Trade Commission ("FTC") guidance respecting protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. The FTC has emphasized the importance of implementing reasonable security systems to protect sensitive customer data.

164. To that end, FTC has expressly recommended that Companies:

i. limit access to customer information to employees who have a business reason to see it;

ii. keep customer information in **encrypted** files to provide better protection in case of theft;

iii. maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;

iv. use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;

[45] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business, last visited August 2, 2024.

v. monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and

vi. monitor activity logs for signs of unauthorized access to customer information.[46]

165. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[47]

166. In 2016, the FTC updated its publication, "Protecting PII: A Guide for Business," which established guidelines for fundamental data security principles and practices for business.[48] The guidelines note that businesses should protect the personal customer information they keep; properly dispose of PII that is no longer needed; **encrypt** information stored on computer networks; understand their network's vulnerabilities; and implement policies to **correct security problems**.

167. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

168. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

---

[46]. https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

[47] Federal Trade Commission, Start With Security at 2, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[48] Federal Trade Commission, Protecting PII: A Guide for Business, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

169. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

170. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.[49] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps data breach victims (like Plaintiffs and Class Members) must take after a data breach are both time-consuming and of only limited and short-term effectiveness.

171. The FTC, like the GAO, recommends several steps that data breach victims should take to protect their personal and financial information after a data breach, including contacting credit bureaus to place a fraud alert and considering an extended fraud alert that lasts for seven years if they have been the victom of identity theft, reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting and errors or discrepancies in their credit reports.[50]

172. Even where a data breach is disclosed promptly, which AT&T failed to do here, there may be a substantial lag—measured in years—between when PII is stolen and when it is used. According to the GAO:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[51]

[49] Government Accountability Off., *Data Breaches* (Mar. 2019) https://www.gao.gov/assets/gao-19-230.pdf (last visited August 2, 2024).

[50] *See Identity Theft Victim Checklist*, Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last visited August 2, 2024).

[51] *See* 2007 GAO Report, at 29.

173. Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of AT&T's failure to adequately protect their PII.

174. The National Institute of Standards and Technology ("NIST") also provides a comprehensive cybersecurity framework that it encourages companies to use to evaluate and improve their cybersecurity protocols.[52]

175. The NIST framework includes substantive recommendations and procedural guidance on a wide range of cybersecurity issues including risk assessment, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[53] Upon information and belief, AT&T failed to implement practices and protocols consistent with NIST guidance.

176. AT&T was aware of its obligations to protect its customers' PII and privacy before and during the Data Breach. In this case, AT&T was at all times fully aware of its obligation to protect the PII of its customers yet failed to take reasonable steps to protect customers' PII from unauthorized access. AT&T was also aware of the risk of significant harm to consumers by its failure to do so because AT&T collected PII from tens of millions of consumers and knew that this PII, if hacked, would result in injury to consumers, including Plaintiffs and Class Members.

177. Beyond the foregoing, AT&T also failed to fully comply with industry-standard cybersecurity practices, including, but not limited to, proper firewall configuration, network segmentation, secure credential storage, rate limiting, user-activity monitoring, data-loss prevention, intrusion detection and prevention and adequate encryption.

CLASS ACTION ALLEGATIONS

178. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure 23(a), (b)(1), (2), (3), and (c)(4) on behalf of the classes defined as follows:

Nationwide Class: *All residents of the United States whose PII was accessed or otherwise*

[52] *See Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, available at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (last visited August 2, 2024).

[53] *Id.* at Table 2 pg. 26-43.

compromised as a result of the Data Breach.

Arkansas Subclass: *All residents of the State of Arkansas whose PII was accessed or otherwise compromised as a result of the Data Breach.*

California Subclass: *All residents of the state of California whose PII was accessed or otherwise compromised as a result of the Data Breach.*

Florida Subclass: *All residents of the State of Florida whose PII was accessed or otherwise compromised as a result of the Data Breach.*

Illinois Subclass: *All residents of the State of Illinois whose PII was accessed or otherwise compromised as a result of the Data Breach.*

New York Subclass: *All residents of the State of New York whose PII was accessed or otherwise compromised as a result of the Data Breach.*

Pennsylvania Subclass: *All residents of the Commonwealth of Pennsylvania whose PII was accessed or otherwise compromised as a result of the Data Breach.*

Texas Subclass: *All residents of the State of Texas whose PII was accessed or otherwise compromised as a result of the Data Breach.*

179. Members of the Nationwide Class, the aforementioned Arkansas, California, Florida Illinois, New York, Pennsylvania, and Texas subclasses (the "State Subclasses") are collectively referred to as "Class Members" and, unless stated otherwise, are referred to collectively as "the Class."

180. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

181. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (2),(3), and (c)(4).

182. **Numerosity:** Each Class is so numerous that joinder of all members is impracticable. Based on information and belief, each Class includes millions of individuals who has had their PII

compromised, stolen, and published during the Data Breach. The parties will be able to identify the exact size of the class through discovery and AT&T's own documents.

183. **Commonality:** There are numerous questions of law and fact common to Plaintiffs and the Class including, but not limited to, the following:

- whether Defendant engaged in the wrongful conduct alleged herein;
- whether Defendant owed a duty to Plaintiffs and members of the Class to adequately protect their personal information;
- whether Defendant breached their duties to protect the personal information of Plaintiffs and Class members;
- whether Defendant knew or should have known that its data security systems, policies, procedures, and practices were vulnerable;
- whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's conduct, including increased risk of identity theft and loss of value of PII;
- whether Defendant violated state consumer protection statutes; and
- whether Plaintiffs and Class Members are entitled to equitable relief including injunctive relief.

184. **Typicality:** Plaintiffs' claims are typical of the claims of the Class members. Plaintiffs, like all Class members, had their personal information compromised in the Data Breach.

185. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no interests that are averse to, or in conflict with the Class Members. There are no claims or defenses that are unique to Plaintiffs. Likewise, Plaintiffs have retained counsel experienced in class action and complex litigation, including data breach litigation, and have sufficient resources to prosecute this action vigorously.

186. **Predominance:** The proposed action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Class predominate over any questions which may affect only individual Class Members.

187. **Superiority:** The proposed action also meets the requirements of Federal Rule of

Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

188. Absent a class action, the majority of Class members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

189. **Risks of Prosecuting Separate Actions:** Plaintiffs' claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendant. Defendant continues to maintain the PII of Class Members and other individuals, and varying adjudications could establish incompatible standards with respect to its duty to protect individuals' PII; and whether the injuries suffered by Class Members are legally cognizable, among others. Prosecution of separate actions by individual Class Members would also create a risk of individual adjudications that would be dispositive of the interests of other class members not parties to the individual adjudications, or substantially impair or impede the ability of Class Members to protect their interests.

190. **Injunctive Relief:** In addition, Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the class under Federal Rule of Civil Procedure 23(b)(2). Defendant continues to (1) maintain the PII of Class members, (2) fail to adequately protect said PII, and (3) violate Class Members' rights under state consumer protection laws and other claims alleged herein.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses against Defendant)

191. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

192. Plaintiffs bring this claim on behalf of themselves and the Class.

193. Plaintiffs and Class Members were required to provide Defendant with their PII. Defendant collected and stored this information including their names, Social Security numbers, email address, mailing address, birth date, and other PII.

194. Defendant had a duty to Plaintiffs and Class Members to safeguard and protect their PII.

195. Defendant assumed a duty of care to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

196. Defendant has full knowledge about the sensitivity of Plaintiffs' and Class Members' PII, as well as the type of harm that would occur if such PII was wrongfully disclosed.

197. Defendant has a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with user PII data.

198. Defendant breached their duty of care by failing to secure and safeguard the PII of Plaintiffs and Class members. Defendant negligently stored and/or maintained its data security systems and published that information on the Internet.

199. Further, Defendant by and through their above negligent actions and/or inactions, breached their duties to Plaintiffs and Class Members by failing to design, adopt, implement, control, manage, monitor, and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' PII within their possession, custody and control.

200. Plaintiffs and the other Class Members have suffered harm as a result of Defendant's negligence. These victims' loss of control over the compromised PII subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, or access to their user accounts.

201. It was reasonably foreseeable – in that Defendant knew or should have known – that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

202. But for Defendants' negligent and wrongful breach of their responsibilities and duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

203. As a direct and proximate result of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm for which they are entitled to compensation. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence/negligent misrepresentation.

204. Plaintiffs and Class Members are entitled to injunctive relief as well as actual and punitive damages.

SECOND CAUSE OF ACTION
Breach of Contract
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses against Defendant)

205. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

206. Plaintiffs and Class Members entered into a contract with Defendant for the provision of title insurance or other closing services.

207. The terms of Defendant's privacy policy are part of the contract it enters with each Class Member to provide wireless services.

208. Plaintiffs and Class Members performed substantially all that was required of them under their contract with Defendant, or they were excused from doing so.

209. Defendant failed to perform its obligations under the contract, including by failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiffs and Class Member's information.

210. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received title insurance or other closing services that were less valuable than described in their contracts. Plaintiffs and Class

Members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendant's deficient performance.

211. Also, as a result of Defendant's breach of contract, Plaintiffs and Class Members have suffered actual damages resulting from the exposure of their personal information, and they remain at imminent risk of suffering additional damages in the future.

212. Accordingly, Plaintiffs and Class Members have been injured by Defendant's breach of contract and are entitled to damages and/or restitution in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses against Defendant)

213. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

214. Defendant received a benefit from Plaintiffs and the Class in the form of payments for title insurance or other closing services.

215. The benefits received by Defendant were at the expense of Plaintiffs and Class Members.

216. The circumstances here are such that it would be unjust for Defendant to retain the portion of Plaintiffs' and Class Members' payments that should have been earmarked to provide adequate privacy, security, and confidentiality safeguards for Plaintiffs' and Class Members' personal information.

217. Plaintiffs and the Class seek disgorgement of Defendant's ill-gotten gains.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses against Defendant)

218. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

219. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of their use of Defendant's services. By providing their PII, and upon Defendant's acceptance of such information, Plaintiffs and Class Members, on one hand, and Defendant, on the

other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contracts.

220. These implied-in-fact contracts obligated Defendant to take reasonable steps to secure and safeguard Plaintiffs' and Class Members' PII. The terms of these implied contracts are further described in the federal laws, state laws, and industry standards alleged above, and Defendant expressly assented to these terms in their Privacy Policy and other public statement described above.

221. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services, along with Defendant's promise to protect their PII from unauthorized disclosure.

222. In its Privacy Policy, Defendant expressly promised Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

223. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide PII was Defendant 's obligation to (a) use such PII for business purposes only; (b) take reasonable steps to safeguard that PII; (c) prevent unauthorized disclosures of the PII; (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses; and (f) retain the PII only under conditions that kept such information secure and confidential.

224. Without such implied contracts, Plaintiffs and Class Members would not have provided their PII to Defendant.

225. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

226. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII, which was compromised as a result of the Data Breach.

227. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the

difference in the value of the secure telecommunication services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiffs and other Class Members have been put at an increased risk of identity theft, fraud, and/or misuse of their PII, which may take months if not years to manifest, discover, and detect.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses against Defendant)

228. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

229. In light of their special relationship, Defendant has become the guardian of Plaintiffs' and Class Members' PII. Defendant has become a fiduciary, created by its undertaking and guardianship of its customers' PII, to act primarily for the benefit of its customers, including Plaintiffs and Class Members. This duty included the obligation to safeguard Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

230. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to properly encrypt and otherwise protect the integrity of the system containing Plaintiffs' and Class Members' PII.

231. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) an increased risk of identity theft, fraud, and/or misuse of their PII; (c) the loss of the opportunity of how their PII is used; (d) the compromise, publication, and/or theft of their PII; (e) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (f) lost opportunity costs associated with the effort

expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (g) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect customers' PII in their continued possession; and (h) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

232. As a direct and proximate result of Defendant's breach of their fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SIXTH CAUSE OF ACTION
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

(On Behalf of the Nationwide Class or Alternatively, the State Subclasses against Defendant)

233. Plaintiffs, individually and on behalf of the Nationwide Class or alternatively the California Subclass, re-allege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

234. Plaintiffs and Class Members entered into valid, binding, and enforceable express or implied contracts with Defendant, as alleged above.

235. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the covenants that Defendant would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiffs' and Class Members' PII and to comply with industry standards and federal and state laws and regulations.

236. A "special relationship" exists between Defendant and the Plaintiffs and Class Members. Defendant entered into a "special relationship" with Plaintiffs and Class Members who entrusted Defendant, pursuant to Defendant's requirements, with their PII.

237. Despite this special relationship with Plaintiffs and Class Members, Defendant did not act in good faith and with fair dealing to protect Plaintiffs' and Class Members' PII.

238. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant.

239. Defendant's failure to act in good faith in implementing the security measures required by the contracts denied Plaintiffs and Class Members the full benefit of their bargain, and instead they received wireless and related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs and Class Members were damaged in an amount at least equal to this overpayment.

240. Defendant's failure to act in good faith in implementing the security measures required by the contracts also caused Plaintiffs and Class Members to suffer actual damages resulting from the theft of their PII, and Plaintiffs and Class Members remain at imminent risk of suffering additional damages in the future.

241. Accordingly, Plaintiffs and Class Members have been injured as a result of Defendant's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

SEVENTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of the Nationwide Class or Alternatively, the State Subclasses against Defendant)

242. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

243. Plaintiffs bring this claim on behalf of themselves and the Class.

244. Plaintiffs and Class Members have a legally protected privacy interest in their PII that Defendant required them to provide and allow them to store.

245. Plaintiffs and Class Members reasonably expected that their PII would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

246. Defendant unlawfully invaded the privacy rights of Plaintiffs and Class Members by (a) failing to adequately secure their PII from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII to unauthorized parties without the informed and clear consent of Plaintiffs and Class members. This invasion into the privacy interest of Plaintiffs and Class Members is serious and substantial.

247. In failing to adequately secure Plaintiffs' and Class Members' PII, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiffs and Class Members.

248. Defendant violated Plaintiffs' and Class Members' right to privacy under the common law as well as under state and federal law.

249. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiffs' and Class Members' PII has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and Class Members have suffered injury as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

EIGHTH CAUSE OF ACTION
Injunctive/Declaratory Relief

(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses against Defendant)

250. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

251. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

252. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII they collected from Plaintiffs and Class Members.

253. Defendant owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure PII.

254. Defendant still possesses PII regarding Plaintiffs and Class Members.

255. Since the Data Breach, Defendant has announced few if any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

256. Defendant has not satisfied their contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

257. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

258. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

259. Plaintiffs therefore seek a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering

Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant not transmit PII via unencrypted email;

f. Ordering that Defendant not store PII in email accounts;

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

h. Ordering that Defendant conduct regular computer system scanning and security checks;

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

CLAIMS AGAINST AT&T ON BEHALF OF THE ARKANSAS SUBCLASS

NINTH CAUSE OF ACTION
ARKANSAS DECEPTIVE TRADE PRACTICES ACT, A.C.A. §§ 4-88-101, *et seq*.

260. Arkansas Plaintiff Pettus ("Plaintiff," for purposes of this Count), individually and on behalf of the Arkansas Subclass, repeats and realleges the allegations above as if fully set forth herein.

261. AT&T is a "person" as defined by A.C.A. § 4-88-102(5). 298. AT&T's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

262. AT&T advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

263. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. §§ 4-88-101, *et seq*., prohibits unfair, deceptive, false, and unconscionable trade practices.

264. AT&T engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of A.C.A. § 4-88-1-8(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services or as to whether goods are original or new or of a particular standard, quality, grade, style, or model;

b. Advertising the goods or services with the intent not to sell them as advertised;

c. Employing bait-and-switch advertising consisting of an attractive but insincere offer to sell a product or service which the seller in truth does not intend or desire to sell;

d. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest;

e. Engaging in any other unconscionable, false, or deceptive act or practice in business, commerce, or trade.

265. AT&T's unconscionable, false, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; and

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII.

266. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

267. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' PII.

268. AT&T intended to mislead Plaintiff and Arkansas Subclass Members and induce them to rely on its misrepresentations and omissions.

269. Had AT&T disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, AT&T would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. AT&T was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. AT&T accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on AT&T's misrepresentations and omissions, the truth of which they could not have discovered.

270. AT&T acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Arkansas Subclass Members' rights. AT&T's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

271. As a direct and proximate result of AT&T's unconscionable, unfair, and deceptive acts or practices and Plaintiff and Arkansas Subclass Members' reliance thereon, Plaintiff and Arkansas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for AT&T's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

272. Plaintiff and the Arkansas Subclass Members seek all monetary and nonmonetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS AGAINST AT&T ON BEHALF OF THE CALIFORNIA SUBCLASS

TENTH CAUSE OF ACTION
CALIFORNIA CONSUMER PRIVACY ACT ("CCPA"), Cal. Civ. Code §§ 1798.150, *et seq.*

273. California Plaintiff Castro ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the allegations set forth above as if fully set forth herein.

274. Plaintiff and Subclass Members are residents of California.

275. AT&T is a corporation organized or operated for the profit or financial benefit of its owners with annual gross revenues over $80 billion. Defendant collects consumers' personal information ("PII" for purposes of this Count) as defined in Cal. Civ. Code § 1798.140.

276. AT&T violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and the Subclass Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of

AT&T's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

277. AT&T has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and Subclass Members' PII. As detailed herein, AT&T failed to do so.

278. As a direct and proximate result of AT&T's acts, Plaintiff's and Subclass Members' PII, including social security numbers, phone numbers, names, addresses, unique IMEI numbers, and driver's license information, was subjected to unauthorized access and exfiltration, theft, or disclosure.

279. Plaintiff and Subclass Members seek injunctive or other equitable relief to ensure AT&T hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because AT&T continues to hold customers' PII, including Plaintiff's and Subclass Members' PII. Plaintiff and Subclass Members have an interest in ensuring that their PII is reasonably protected, and AT&T has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by its multiple data breaches.

280. Pursuant to Cal. Civ. Code § 1798.150(b), on August 25, 2021, Plaintiff mailed CCPA notice letter to Defendant's registered service agents via overnight post, detailing the specific provisions of the CCPA that AT&T has and continues to violate. AT&T did not cure within 30 days.

281. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the PII under the CCPA.

282. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

283. Plaintiff and the California Subclass seek statutory damages of between $100 and $750 per customer per violation or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

ELEVENTH CAUSE OF ACTION
CALIFORNIA CUSTOMER RECORDS ACT,
Cal. Civ. Code §§ 1798.80, *et seq.*

284. California Plaintiff Castro ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the allegations set forth above as if fully set forth herein.

285. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PII from unauthorized access, destruction, use, modification, or disclosure."

286. AT&T is a business that owns, maintains, and licenses personal information (or "PII"), within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass Members.

287. Businesses that own or license computerized data that includes PII, including Social Security numbers, are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of PII that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

288. AT&T is a business that owns or licenses computerized data that includes PII as defined by Cal. Civ. Code § 1798.82.

289. Plaintiff and California Subclass Members' PII (e.g., Social Security numbers) includes PII as covered by Cal. Civ. Code § 1798.82.

290. Because AT&T reasonably believed that Plaintiff's and California Subclass Members' PII was acquired by unauthorized persons during the AT&T data breach, AT&T had an obligation to disclose the AT&T data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

291. AT&T failed to fully disclose material information about the Data Breach, including the types of PII impacted.

292. By failing to disclose the AT&T data breach in a timely and accurate manner, AT&T violated Cal. Civ. Code § 1798.82.

293. As a direct and proximate result of AT&T's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass Members suffered damages, as described above. 331. Plaintiff and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

TWELTH CAUSE OF ACTION
CALIFORNIA UNFAIR COMPETITION ACT,
Cal. Bus. & Prof. Code §§ 17200, *et seq*.

294. California Plaintiff Castro ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the allegations set forth above as if fully set forth herein.

295. AT&T is a "person" as defined by Cal. Bus. & Prof. Code §17201. 334. AT&T violated Cal. Bus. & Prof. Code §§ 17200, *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

296. AT&T's "unfair" acts and practices include:

a. AT&T failed to implement and maintain reasonable security measures to protect Plaintiff and Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. AT&T failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and Class members, whose PII has been compromised.

c. AT&T's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's

Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

d. AT&T's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of AT&T's grossly inadequate security, consumers could not have reasonably avoided the harms that AT&T caused.

e. AT&T engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

297. AT&T has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, and California common law.

298. AT&T's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, California's Consumer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*. and 1798.81.5, which was a direct and proximate cause of the Data Breach.

299. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' PII.

300. As a direct and proximate result of AT&T's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for AT&T's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

301. AT&T acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and California Subclass Members' rights. AT&T's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

302. Plaintiff and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from AT&T's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs

under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

THIRTEENTH CAUSE OF ACTION
CALIFORNIA CONSUMER LEGAL REMEDIES ACT,
Cal. Civ. Code §§ 1750, *et seq*.

303. California Plaintiff Castro ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the allegations set forth above as if fully set forth herein.

304. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

305. AT&T is a "person" as defined by Civil Code §§ 1761(c) and 1770 and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

306. Plaintiff and the California Subclass are "consumers" as defined by Civil Code §§ 1761(d) and 1770 and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

307. AT&T's acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass Members in violation of Civil Code § 1770, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

308. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' PII.

309. Had AT&T disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, AT&T would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. AT&T was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. AT&T accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on AT&T's misrepresentations and omissions, the truth of which they could not have discovered.

310. As a direct and proximate result of AT&T's violations of California Civil Code § 1770, Plaintiff and California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for AT&T's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

311. The unfair and deceptive acts and practices of Defendant, as described above, present a serious threat to Plaintiff and members of the Nationwide Class.

312. Plaintiff seeks equitable relief and an order enjoining Defendant's unfair or deceptive acts or practices under California Civil Code § 1780(e).

313. Plaintiff and Nationwide Class members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

CLAIMS AGAINST AT&T ON BEHALF OF THE FLORIDA SUBCLASS

FOURTEENTH CAUSE OF ACTION
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, *et seq*.

314. Florida Plaintiff Hamilton ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, repeats and realleges the allegations set forth above as if fully set forth herein.

315. Plaintiff and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

316. AT&T advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

317. AT&T engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

318. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' PII.

319. Had AT&T disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, AT&T would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. AT&T was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. AT&T accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on AT&T's misrepresentations and omissions, the truth of which they could not have discovered.

320. As a direct and proximate result of AT&T's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for AT&T's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

321. Plaintiff and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief;

reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS AGAINST AT&T ON BEHALF OF THE ILLINOIS SUBCLASS

FIFTHEENTH CAUSE OF ACTION
ILLINOIS PERSONAL INFORMATION PROTECTION ACT, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*.

322. Illinois Plaintiff Palafox ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and realleges the allegations set forth above as if fully set forth herein.

323. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information (for the purpose of this count, "PII"), AT&T is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

324. Plaintiff and Illinois Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under 815 Ill. Comp. Stat. § 530/5.

325. As a Data Collector, AT&T is required to notify Plaintiff and Illinois Subclass Members of a breach of its data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

326. By failing to disclose the AT&T data breach in the most expedient time possible and without unreasonable delay, AT&T violated 815 Ill. Comp. Stat. § 530/10(a).

327. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

328. As a direct and proximate result of AT&T's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Illinois Subclass Members suffered damages, as described above.

329. Plaintiff and Connecticut Subclass Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of AT&T's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

SIXTEENTH CAUSE OF ACTION
ILLINOIS CONSUMER FRAUD ACT,
815 Ill. Comp. Stat. §§ 505, *et seq*.

330. Illinois Plaintiff Palafox ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and realleges the allegations set forth above as if fully set forth herein.

331. AT&T is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

332. Plaintiff and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

333. AT&T's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

334. AT&T's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

335. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' PII.

336. AT&T intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

337. The above unfair and deceptive practices and acts by AT&T were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

338. AT&T acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass Members' rights. AT&T's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

339. As a direct and proximate result of AT&T's unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for AT&T's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach. 509. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

SEVENTEENTH CAUSE OF ACTION
ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 Ill. Comp. Stat. §§ 510/2, *et seq*.

340. Illinois Plaintiff Palafox ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and realleges the allegations set forth above as if fully set forth herein.

341. AT&T is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

342. AT&T engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

343. AT&T's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs'

and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

344. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' PII.

345. The above unfair and deceptive practices and acts by AT&T were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

346. As a direct and proximate result of AT&T's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for AT&T's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

347. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

CLAIMS AGAINST AT&T ON BEHALF OF THE NEW YORK SUBCLASS

EIGHTEENTH CAUSE OF ACTION
NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349, *et seq*.

348. New York Plaintiff Gilsey ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeats and realleges the allegations set forth above as if fully set forth herein.

349. AT&T engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

350. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' PII.

351. AT&T acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass Members' rights. AT&T's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

352. As a direct and proximate result of AT&T's deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for AT&T's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

353. AT&T's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the AT&T Data Breach.

354. The above deceptive and unlawful practices and acts by AT&T caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably avoid.

355. Plaintiff and New York Subclass Members seek seek all monetary and nonmonetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

CLAIMS AGAINST AT&T ON BEHALF OF THE PENNSYLVANIA SUBCLASS

NINETEENTH CAUSE OF ACTION
PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW,
73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq*.

356. Pennsylvania Plaintiff Young ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeats and realleges the allegations set forth above as if fully set forth herein.

357. AT&T is a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

358. Plaintiff and Pennsylvania Subclass Members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

359. AT&T engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201- 2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

360. AT&T's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

361. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' PII.

362. AT&T intended to mislead Plaintiff and Pennsylvania Subclass Members and induce them to rely on its misrepresentations and omissions.

363. Had AT&T disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, AT&T would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. AT&T was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. AT&T accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on AT&T's misrepresentations and omissions, the truth of which they could not have discovered.

364. AT&T acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass Members' rights. AT&T's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

365. As a direct and proximate result of AT&T's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass' reliance on them, Plaintiff and Pennsylvania Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for AT&T's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

366. Plaintiff and Pennsylvania Subclass Members seek all monetary and nonmonetary relief allowed by law, including, pursuant to 73 Pa. Stat. Ann. § 201-9.2, actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request that the Court enter a judgment awarding the following relief:

a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Nationwide Class and State Subclasses requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class and State Subclasses requested herein;

b. Declaratory relief requiring Defendant to (1) strengthen their data security systems that maintain personally identifying information to comply with the applicable state laws alleged herein and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendant's systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

c. An order requiring Defendant to pay all costs associated with class notice and administration of class-wide relief;

d. An award to Plaintiffs and all Class Members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

e. An award to Plaintiffs and all Class Members credit monitoring and identity theft protection services;

f. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

g. An order requiring Defendant to pay pre-judgment and post-judgment interest, as provided by law or equity; and

h. Such other or further relief as the Court may allow.

Dated: August 5, 2024

Respectfully submitted,

STECKLER WAYNE & LOVE PLLC

By: */s/ Bruce W. Steckler*

BRUCE W. STECKLER
12720 Hillcrest Suite 1045
Dallas, Texas 75230
Telephone: (972) 387-4040
Cell: (214) 208-3327
bruce@stecklerlaw.com

BARRACK, RODOS & BACINE
STEPHEN R. BASSER
SAMUEL M. WARD
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874
sbasser@barrack.com
sward@barrack.com

BARRACK, RODOS & BACINE
DANIELLE M. WEISS

Two Commerce Square
2001 Market Street, Suite 3300
Philadelphia, PA 19103
Telephone: (215) 963-0600
dweiss@barrack.com

EMERSON FIRM, PLLC
JOHN G. EMERSON
2500 Wilcrest, Suite 300
Houston, TX 77042
Phone: 800-551-8649
Fax: 501-286-4659
jemerson@emersonfirm.com

Counsel for Plaintiffs
Monique Castro, Andrew Gilsey, Anna Hamilton, Anna Palafox, Latoya Pettus, Tina Salinas, and Tina Young